ÁLGEBRA LINEAR I (BCC)

2º SEMESTRE DE 2024

RESUMO

Observação. Este resumo pode ser útil para rever os conceitos mais importantes vistos nesta disciplina. Não há pretensão de ser um texto completo. Este texto será atualizado e revisado conforme formos avançando no semestre. Correções, perguntas e comentários serão bem-vindos.

* * * * *

§0. Funções e outras coisas básicas

Dados dois conjuntos A e B, denotamos por A^B o conjunto das funções $f\colon B \to A$.

A função *identidade* em A é a função $\mathrm{id}_A\colon A \to A$ tal que $\mathrm{id}_A(a) = a$ para todo $a \in A$. Suponha que $f\colon B \to A$ e $g\colon A \to B$ sejam tais que $f \circ g = \mathrm{id}_A$ e $g \circ f = \mathrm{id}_B$. Dizemos então que f e g são funções *inversas* uma da outra. Se f admite uma função inversa, então ela é única. Escrevemos f^{-1} para tal inversa.

Uma função $f\colon A \to B$ admite uma inversa se e só se f for injetora e sobrejetora.

§1. Corpos

Nesta disciplina, trabalhamos com os corpos $\mathbb{R}$, $\mathbb{C}$ e $\mathrm{GF}(2)$. Ocasionalmente, poderemos também considerar o corpo $\mathbb{Q}$ ou o corpo $\mathbb{Z}/p\mathbb{Z}$ dos inteiros módulo p. Escrevemos $\mathbb{F}$ para denotar o corpo sobre o qual estamos trabalhando.

§2. Vetores

Nesta disciplina, em geral, quando dizemos que $\mathbf{v}$ é um vetor, temos um corpo $\mathbb{F}$ e um conjunto D fixo, e $\mathbf{v} \in \mathbb{F}^D$. Ademais, os elementos de $\mathbb{F}$ são chamados de *escalares*. Em geral, D será um conjunto finito e apenas ocasionalmente consideraremos o caso em que D não é finito.

2.1. **Operações com vetores.** Sejam $\mathbf{u}$ e $\mathbf{v}$ vetores em $\mathbb{F}^D$ e α um escalar (isto é, $\alpha \in \mathbb{F}$). A soma $\mathbf{u} + \mathbf{v}$ dos vetores $\mathbf{u}$ e $\mathbf{v}$ é o vetor em $\mathbb{F}^D$ tal que $(\mathbf{u} + \mathbf{v})(d) = \mathbf{u}(d) + \mathbf{v}(d)$ para todo $d \in D$. O produto $\alpha\mathbf{u}$ é o vetor em $\mathbb{F}^D$ dado por $(\alpha\mathbf{u})(d) = \alpha\mathbf{u}(d)$ para todo $d \in D$. (Essa é a forma usual de se definir a soma de duas funções com o mesmo domínio ("soma ponto a ponto") e produto de funções por escalares.)

Finalmente, definimos o *produto escalar* ou *produto interno* $\mathbf{u} \cdot \mathbf{v}$ (*dot-product*) de $\mathbf{u}$ e $\mathbf{v}$ como sendo o escalar

$$\sum_{d \in D} \mathbf{u}(d)\mathbf{v}(d). \tag{1}$$

Produtos escalares podem ser definidos de forma mais geral. Assim, o produto escalar que acabamos de definir é às vezes chamado de produto escalar *padrão*.

Date: Versão de 2025/2/9, 5:08pm.

§3. Espaços vetoriais

3.1. **Combinações lineares.** Dados vetores $\mathbf{v}_1, \ldots, \mathbf{v}_n$ e escalares $\alpha_1, \ldots, \alpha_n$, podemos considerar a *combinação linear*

$$\alpha_1 \mathbf{v}_1 + \cdots + \alpha_n \mathbf{v}_n. \tag{2}$$

3.2. **Espaços gerados.** Dados vetores $\mathbf{v}_1, \ldots, \mathbf{v}_n$, o conjunto

$$\operatorname{Span}\{\mathbf{v}_1, \ldots, \mathbf{v}_n\} = \Big\{ \sum_{1 \le i \le n} \alpha_i \mathbf{v}_i \colon \alpha_i \in \mathbb{F} \text{ para todo } i \Big\} \tag{3}$$

das combinações lineares dos $\mathbf{v}_i$ é o *espaço gerado* por esses vetores.

3.3. **Variedades lineares (flats) contendo 0.** Certos conjuntos de vetores são chamados de variedades lineares (flats). Consideramos aqui variedades lineares que contém $\mathbf{0}$. Um conjunto $U \subset \mathbb{F}^D$ é uma *variedade linear* (ou *flat*) *que contém* $\mathbf{0}$ se valem as seguintes três propriedades:

(V1) $\mathbf{0} \in U$,

(V2) $\mathbf{u} + \mathbf{v} \in U$ sempre que $\mathbf{u} \in U$ e $\mathbf{v} \in U$, e

(V3) $\alpha \mathbf{v} \in U$ sempre que $\alpha \in \mathbb{F}$ e $\mathbf{v} \in U$.

3.3.1. *Espaços gerados por vetores.* Sejam $\mathbf{v}_i$ $(1 \le i \le n)$ vetores quaisquer e considere $S = \operatorname{Span}\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$. Note que S satisfaz (V1), (V2) e (V3) acima e assim S é uma variedade linear que contém $\mathbf{0}$.

3.3.2. *Espaço das soluções de sistemas lineares homogêneos.* Sejam dados $\mathbf{a}_i \in \mathbb{F}^D$ $(1 \le i \le n)$ e considere o sistema de equações lineares homogêneas[1]

$$\begin{cases} \mathbf{a}_1 \cdot \mathbf{x} = 0 \\ \quad \ldots \\ \mathbf{a}_n \cdot \mathbf{x} = 0. \end{cases} \tag{4}$$

Seja $T = \{\mathbf{x} \in \mathbb{F}^D \colon \mathbf{x} \text{ satisfaz } (4)\}$ o conjunto das soluções de (4). Note que T satisfaz (V1), (V2) e (V3) e assim T é uma variedade linear que contém $\mathbf{0}$.

3.4. **Espaços vetoriais.** Nesta disciplina, definimos *espaços vetoriais* como sendo variedades lineares contidas em $\mathbb{F}^D$ que contém $\mathbf{0}$. Dizemos que tais espaços vetoriais são espaços vetoriais *sobre* $\mathbb{F}$. Os conjuntos S e T de §3.3.1 e §3.3.2 são portanto espaços vetoriais sobre $\mathbb{F}$.

Observação. Em certas ocasiões, teremos conjuntos V que podem ser identificados com os espaços vetoriais definidos acima. Nesses casos, vamos também nos referir a tais conjuntos como espaços vetoriais.

Exemplo 3.4.1. Seja V o conjunto dos polinômios de grau no máximo 3 com coeficientes em $\mathbb{F}$, munido com as operações de soma de polinômios e produto por escalar usuais: se $p(X) = a_0 + a_1 X + a_2 X^2 + a_3 X^3$ e $q(X) = b_0 + b_1 X + b_2 X^2 + b_3 X^3$ então

$$p(X) + q(X) = (a_0 + b_0) + (a_1 + b_1)X + (a_2 + b_2)X^2 + (a_3 + b_3)X^3 \tag{5}$$

e se $\alpha \in \mathbb{F}$ então

$$\alpha p(X) = \alpha a_0 + \alpha a_1 X + \alpha a_2 X^2 + \alpha a_3 X^3. \tag{6}$$

[1] Equações lineares *homogêneas* são equações da forma $\mathbf{a} \cdot \mathbf{x} = \beta$ com $\beta = 0$.

Então V pode ser naturalmente identificado com $\mathbb{F}^4$ e assim V é um espaço vetorial sobre $\mathbb{F}$.

3.4.1. *Subespaços vetoriais.* Sejam U e V espaços vetoriais, com $U \subset V$. Dizemos então que U é um *subespaço* vetorial de V.

3.4.2. *Espaços vetoriais abstratos.* Em um tratamento mais geral de álgebra linear, definimos espaços vetoriais sobre um corpo $\mathbb{F}$ como sendo triplas $(V, +, \cdot)$, onde V é um conjunto arbitrário e $+\colon V \times V \to V$ (soma de elementos de V) e $\cdot\colon \mathbb{F} \times V \to V$ (multiplicação de elementos de V por escalares) são operações que satisfazem certos axiomas (veja, por exemplo esta página).

Nesta disciplina, o conjunto V na definição acima será sempre um subconjunto de $\mathbb{F}^D$ para algum D finito que satisfaz (V1), (V2) e (V3) (ou V pode ser naturalmente identificado com um tal subconjunto), e assim adotamos nossa definição bem mais restrita. Do ponto de vista computacional, sempre trabalharemos com tais V concretos.

3.5. **Espaços afins.** Consideramos até agora variedades lineares que contém $\mathbf{0}$, e denominamos tais variedades de espaços vetoriais. Uma variedade linear geral não necessariamente contém $\mathbf{0}$. Definimos uma *variedade linear* como sendo conjuntos de vetores da forma

$$\mathbf{u} + V = \{\mathbf{u} + \mathbf{v}\colon \mathbf{v} \in V\}, \tag{7}$$

onde V é um espaço vetorial. Variedades lineares são também conhecidas como *espaços afins*.

3.5.1. *Fecho afim.* Sejam $\mathbf{w}_0, \dots, \mathbf{w}_n$ vetores em um espaço vetorial e sejam $\beta_0, \dots, \beta_n$ escalares. A combinação linear

$$\sum_{0 \le i \le n} \beta_i \mathbf{w}_i \tag{8}$$

é uma *combinação linear afim* dos $\mathbf{w}_i$ $(0 \le i \le n)$ se $\sum_{0 \le i \le n} \beta_i = 1$. O *fecho afim* dos vetores $\mathbf{w}_i$ $(0 \le i \le n)$ é o conjunto

$$\operatorname{Aff}\{\mathbf{w}_0, \dots, \mathbf{w}_n\} = \Big\{ \sum_{0 \le i \le n} \beta_i \mathbf{w}_i\colon \beta_0 + \cdots + \beta_n = 1 \Big\} \tag{9}$$

das combinações afins dos $\mathbf{w}_i$ $(0 \le i \le n)$.

Exemplo 3.5.1. Sejam $\mathbf{w}_0$ e $\mathbf{w}_1$ dois pontos distintos em $\mathbb{R}^2$ ou $\mathbb{R}^3$. Então $\operatorname{Aff}\{\mathbf{w}_0, \mathbf{w}_1\}$ é a reta determinada por esses pontos. Sejam agora $\mathbf{w}_0$, $\mathbf{w}_1$ e $\mathbf{w}_2$ três pontos no $\mathbb{R}^3$, não colineares. Então $\operatorname{Aff}\{\mathbf{w}_0, \mathbf{w}_1, \mathbf{w}_2\}$ é o plano determinado por esses pontos.

Proposição 3.5.2. *Sejam* $\mathbf{u}$ *e* $\mathbf{v}_1, \dots, \mathbf{v}_n$ *vetores em* $\mathbb{F}^D$*. Então*

$$\mathbf{u} + \operatorname{Span}\{\mathbf{v}_1, \dots, \mathbf{v}_n\} = \operatorname{Aff}\{\mathbf{u}, \mathbf{u} + \mathbf{v}_1, \dots, \mathbf{u} + \mathbf{v}_n\}. \tag{10}$$

Equivalentemente, se $\mathbf{w}_0, \dots, \mathbf{w}_n$ *são vetores em* $\mathbb{F}^D$*, então*

$$\operatorname{Aff}\{\mathbf{w}_0, \dots, \mathbf{w}_n\} = \mathbf{w}_0 + \operatorname{Span}\{\mathbf{w}_1 - \mathbf{w}_0, \dots, \mathbf{w}_n - \mathbf{w}_0\}. \tag{11}$$

□

Corolário 3.5.3. *Fechos afins são espaços afins.*

Prova. A identidade (11) diz que fechos afins são da forma (7), isto é, são espaços afins, pois espaços da forma $\operatorname{Span}\{\mathbf{x}_1, \dots, \mathbf{x}_n\}$ são espaços vetoriais. □

3.5.2. *Sistemas lineares homogêneos e não-homogêneos.* Considere o sistema de equações lineares homogêneas (4). Sejam dados agora $\beta_i \in \mathbb{F}$ $(1 \leq i \leq n)$, e considere o sistema (S) dado por

$$(S) \quad \begin{cases} \mathbf{a}_1 \cdot \mathbf{x} = \beta_1 \\ \quad \dots \\ \mathbf{a}_n \cdot \mathbf{x} = \beta_n, \end{cases} \tag{12}$$

onde $\mathbf{x} = (x_d)_{d \in D}$ é o vetor de indeterminadas (lembre que $\mathbf{a}_i \in \mathbb{F}^D$ para todo $1 \leq i \leq n$). O sistema (4) é o *sistema linear homogêneo associado* ao sistema (S) acima. Chamemos o sistema (4) de (H) (de homogêneo).

Proposição 3.5.4. *Suponha que $\mathbf{u}_1 \in \mathbb{F}^D$ seja uma solução de (S) e seja $\mathbf{u}_2 \in \mathbb{F}^D$. São equivalentes*:

(*i*) $\mathbf{u}_2$ *é solução de* (S),

(*ii*) $\mathbf{u}_2 - \mathbf{u}_1$ *é solução de* (H).

□

Sejam

$$U = \{\mathbf{u} \colon \mathbf{u} \text{ é solução de } (S)\} \tag{13}$$

e

$$T = \{\mathbf{v} \colon \mathbf{v} \text{ é solução de } (H)\}. \tag{14}$$

Sabemos que T é um espaço vetorial (veja §3.3.2).

Teorema 3.5.5. *Há duas possibilidades para U*:

(*i*) $U = \emptyset$ *ou*

(*ii*) $U = \mathbf{u} + T$, *onde* $\mathbf{u}$ *é uma solução de* (S).

Em particular, se U é não-vazio, então U é um espaço afim. □

Corolário 3.5.6. *Se (S) admite solução, então ela é única se e só se (H) admite apenas a solução* $\mathbf{0}$. *Mais geralmente, o número de soluções de (S) é zero ou é igual ao número de soluções de (H).*

Corolário 3.5.7. *O conjunto de soluções de um sistema linear ou é vazio ou é um espaço afim.*

3.6. **Fechos convexos.** Sejam $\mathbf{w}_0, \dots, \mathbf{w}_n$ vetores em $\mathbb{F}^D$, com $\mathbb{F} = \mathbb{R}$ ou $\mathbb{C}$ e sejam $\beta_0, \dots, \beta_n$ escalares. A combinação linear

$$\sum_{0 \leq i \leq n} \beta_i \mathbf{w}_i \tag{15}$$

é uma *combinação convexa* dos $\mathbf{w}_i$ $(0 \leq i \leq n)$ se $\sum_{0 \leq i \leq n} \beta_i = 1$ e $\beta_i \geq 0$ para todo $0 \leq i \leq n$. O *fecho convexo* dos vetores $\mathbf{w}_i$ $(0 \leq i \leq n)$ é o conjunto

$$\mathrm{Conv}\{\mathbf{w}_0, \dots, \mathbf{w}_n\} = \Big\{ \sum_{0 \leq i \leq n} \beta_i \mathbf{w}_i \colon \beta_0 + \dots + \beta_n = 1 \text{ e } \beta_i \geq 0 \text{ para todo } 0 \leq i \leq n \Big\} \tag{16}$$

das combinações convexas dos $\mathbf{w}_i$ $(0 \leq i \leq n)$.

Exemplo 3.6.1. Sejam $\mathbf{w}_0$ e $\mathbf{w}_1$ dois pontos distintos em $\mathbb{R}^2$ ou $\mathbb{R}^3$. Então $\mathrm{Conv}\{\mathbf{w}_0, \mathbf{w}_1\}$ é o segmento de reta com extremos $\mathbf{w}_0$ e $\mathbf{w}_1$. Sejam agora $\mathbf{w}_0$, $\mathbf{w}_1$ e $\mathbf{w}_2$ três pontos no $\mathbb{R}^2$ ou no $\mathbb{R}^3$, não colineares. Então $\mathrm{Conv}\{\mathbf{w}_0, \mathbf{w}_1, \mathbf{w}_2\}$ é o triângulo com vértices $\mathbf{w}_0$, $\mathbf{w}_1$ e $\mathbf{w}_2$.

§4. Matrizes

4.1. **Matrizes como funções.** Sejam R e C conjuntos finitos e $\mathbb{F}$ um corpo. Uma matriz com *linhas indexadas por* R e *colunas indexadas por* C é um elemento de $\mathbb{F}^{R\times C}$.

Seja $M \in \mathbb{F}^{R\times C}$ uma matriz. Para cada $r \in R$, temos a *linha* $M(r, \cdot)\colon C \to \mathbb{F}$ que leva c em $M(r, c)$ para todo $c \in C$. Analogamente, para cada $c \in C$, temos a *coluna* $M(\cdot, c)\colon R \to \mathbb{F}$ que leva r em $M(r, c)$ para todo $r \in R$.

Podemos denotar a linha $M(r, \cdot)$ por M_{r*} e a coluna $M(\cdot, c)$ por M_{*c}.

4.1.1. *Transposta.* Dada uma matriz $M \in \mathbb{F}^{R\times C}$, definimos a *transposta* de M como sendo $M^\top \in \mathbb{F}^{C\times R}$ dada por $M^\top(c, r) = M(r, c)$ para todo $(c, r) \in C \times R$. Quando $M^\top = M$, dizemos que M é *simétrica*.

4.2. **Espaço das matrizes.** Note que as matrizes M em $\mathbb{F}^{R\times C}$ formam um espaço vetorial sobre $\mathbb{F}$: basta considerar $R \times C$ como um sendo conjunto D e pensar em M como sendo um membro de $\mathbb{F}^D = \mathbb{F}^{R\times C}$.

4.3. **Espaço das linhas e espaço das colunas.** Dada uma matriz $M \in \mathbb{F}^{R\times C}$, o espaço

$$\operatorname{Span}\{M_{r*}\colon r \in R\} \subset \mathbb{F}^C \tag{17}$$

gerado pelas linhas M_{r*} $(r \in R)$ de M é o *espaço das linhas* de M. Analogamente,

$$\operatorname{Span}\{M_{*c}\colon c \in C\} \subset \mathbb{F}^R \tag{18}$$

é o *espaço das colunas* de M.

4.4. **Produtos matriz-vetor e vetor-matriz.** Seja $M \in \mathbb{F}^{R\times C}$ uma matriz. Sejam também $\mathbf{u} \in \mathbb{F}^R$ e $\mathbf{v} \in \mathbb{F}^C$. Definimos os *produtos* $\mathbf{u} * M \in \mathbb{F}^C$ e $M * \mathbf{v} \in \mathbb{F}^R$ pondo

$$(\mathbf{u} * M)(c) = \sum_{r\in R} \mathbf{u}(r)M(r, c) \tag{19}$$

para todo $c \in C$ e

$$(M * \mathbf{v})(r) = \sum_{c\in C} M(r, c)\mathbf{v}(c) \tag{20}$$

para todo $r \in R$.

4.4.1. *Interpretações úteis dos produtos.* Sejam $M \in \mathbb{F}^{R\times C}$, $\mathbf{u} \in \mathbb{F}^R$ e $\mathbf{v} \in \mathbb{F}^C$. Temos:

(*i*) $\mathbf{u} * M$ é a combinação linear $\sum_{r\in R} \mathbf{u}(r)M_{r*}$ das linhas M_{r*} de M. Assim, $\mathbf{u} * M$ pertence ao espaço das linhas de M.

(*ii*) $M * \mathbf{v}$ é a combinação linear $\sum_{c\in C} \mathbf{v}(c)M_{*c}$ das colunas M_{*c} de M. Assim, $M * \mathbf{v}$ pertence ao espaço das colunas de M.

Valem também:

(*iii*) $\mathbf{u} * M$ tem como entradas os produtos internos $\mathbf{u} \cdot M_{*c}$ $(c \in C)$; isto é, $(\mathbf{u} * M)(c) = \mathbf{u} \cdot M_{*c}$.

(*iv*) $M * \mathbf{v}$ tem como entradas os produtos internos $M_{r*} \cdot \mathbf{v}$ $(r \in R)$; isto é, $(M * \mathbf{v})(r) = M_{r*} \cdot \mathbf{v}$.

4.4.2. *Sistemas lineares.* Considere o sistema linear (S) em (12). Seja $R = \{1, \dots, n\}$. Lembre que $\mathbf{a}_i \in \mathbb{F}^D$ $(1 \le i \le n)$ e $\mathbf{x} = (x_d)_{d\in D}$ é o vetor das indeterminadas de (S). Monte a matriz $M \in \mathbb{F}^{R\times D}$ cuja i-ésima linha é $\mathbf{a}_i$ $(i \in R)$. Então (S) é equivalente a resolver a equação $M * \mathbf{x} = \boldsymbol{\beta}$, onde $\boldsymbol{\beta} = (\beta_i)_{i\in R}$ (veja (*iv*) acima).

Lembrando (*ii*) acima, a observação do parágrafo anterior implica que resolver o sistema (12) equivale a encontrar coeficientes adequados para escrever $\boldsymbol{\beta}$ como combinação linear das colunas de M. Em particular, o sistema (S) tem solução se e só se $\boldsymbol{\beta}$ pertence ao espaço das colunas de M, isto é, se e só se $\boldsymbol{\beta} \in \operatorname{Span}\{M_{*d} \colon d \in D\}$.

4.5. **Produto matriz-matriz.** Sejam R, C e D conjuntos finitos e sejam $A \in \mathbb{F}^{R\times C}$ e $B \in \mathbb{F}^{C\times D}$ matrizes. O *produto* $A * B$ de A e B é a matriz em $\mathbb{F}^{R\times D}$ com

$$(A * B)(r,d) = \sum_{c\in C} A(r,c)B(c,d) \tag{21}$$

para todo $(r,d) \in R \times D$.

4.5.1. *Interpretações alternativas.* Sejam A e B como acima. O produto $A * B$ acima pode ser pensado de formas alternativas:

(*i*) $A * B$ é a matriz cuja r-ésima linha é $A_{r*} * B$ $(r \in R)$,
(*ii*) $A * B$ é a matriz cuja d-ésima coluna é $A * B_{*d}$ $(d \in D)$ e
(*iii*) $A * B$ é a matriz com $(AB)(r,d) = A_{r*} \cdot B_{*d}$ $((r,d) \in R \times D)$.

4.5.2. *Transposta do produto.* Sejam A e B como acima. Então $(A * B)^\top = B^\top * A^\top$.

4.6. **Notação de produto e vetores-coluna.** Tradicionalmente, o símbolo $*$ não é usado para denotar produtos de vetores e matrizes. A partir de agora vamos omitir $*$ em nossos produtos de vetores e matrizes.

Tradicionalmente, vetores em $\mathbb{F}^d$ são denotados como matrizes $d \times 1$, isto é, como *vetores-coluna*. Podemos adotar a convenção que vetores são vetores-coluna dentro do formalismo que temos. Para tanto, vamos pensar em $\mathbf{v} \in \mathbb{F}^D$ como sendo uma matriz em $\mathbb{F}^{D\times\{1\}}$.

Seja $M \in \mathbb{F}^{R\times C}$ uma matriz e sejam $\mathbf{u} \in \mathbb{F}^R$ e $\mathbf{v} \in \mathbb{F}^C$ vetores. O produto $M * \mathbf{v}$ (veja (20)) pode ser pensado como o produto de matrizes $M\mathbf{v}$, onde o vetor $\mathbf{v}$ é considerado como uma matriz em $\mathbb{F}^{C\times\{1\}}$. Analogamente, o produto $\mathbf{u}*M$ (veja (19)) pode ser pensado como o produto de matrizes $\mathbf{u}^\top M$, onde $\mathbf{u}$ é considerado como uma matriz em $\mathbb{F}^{R\times\{1\}}$ (note que, no produto, usamos a transposta $\mathbf{u}^\top \in \mathbb{F}^{\{1\}\times R}$).

Finalmente, suponha que $\mathbf{x}$ e $\mathbf{y}$ sejam vetores em $\mathbb{F}^D$. Podemos pensar no produto interno $\mathbf{x}\cdot\mathbf{y}$ entre eles como sendo o produto de matrizes $\mathbf{y}^\top\mathbf{x}$ ou $\mathbf{x}^\top\mathbf{y}$.

4.7. **A linearidade de aplicação $\mathbf{v} \mapsto A\mathbf{v}$ e $\operatorname{Null} A$.** Seja A uma matriz em $\mathbb{F}^{R\times C}$. Podemos considerar a função $f_A \colon \mathbb{F}^C \to \mathbb{F}^R$ que leva $\mathbf{v} \in \mathbb{F}^C$ em $f_A(\mathbf{v}) = A\mathbf{v} \in \mathbb{F}^R$ para todo $\mathbf{v} \in \mathbb{F}^C$. Essa aplicação é *linear*, isto é,

(L1) $f_A(\alpha\mathbf{v}) = \alpha f_A(\mathbf{v})$ para todo $\alpha \in \mathbb{F}$ e $\mathbf{v} \in \mathbb{F}^C$ e
(L2) $f_A(\mathbf{v}+\mathbf{w}) = f_A(\mathbf{v}) + f_A(\mathbf{w})$ para todo $\mathbf{v}$ e $\mathbf{w}$ em $\mathbb{F}^C$.

A imagem inversa de $\{\mathbf{0}\}$ pela função f_A é o *espaço nulo* $\operatorname{Null} A$ de A:

$$\operatorname{Null} A = f_A^{-1}(\{\mathbf{0}\}) = \{\mathbf{v} \in \mathbb{F}^C \colon f_A(\mathbf{v}) = \mathbf{0}\} = \{\mathbf{v} \in \mathbb{F}^C \colon A\mathbf{v} = \mathbf{0}\}. \tag{22}$$

Note que $\operatorname{Null} A$ nada mais é que o espaço das soluções do sistema linear homogêneo $A\mathbf{x} = \mathbf{0}$. Assim, aqui estamos apenas dando um nome para um conjunto que já ocorreu em §3.3.2.

Proposição 4.7.1. *Seja A uma matriz em $\mathbb{F}^{R\times C}$ e $\boldsymbol{\beta}$ um vetor em $\mathbb{F}^R$.*

(*i*) *O espaço nulo $\operatorname{Null} A$ de A é um espaço vetorial.*

(*ii*) *O conjunto das soluções do sistema linear* $A\mathbf{x} = \boldsymbol{\beta}$ *é vazio, ou é da forma* $\mathbf{u} + \operatorname{Null} A$*, onde* $\mathbf{u}$ *é qualquer solução de* $A\mathbf{x} = \boldsymbol{\beta}$*.*

4.8. **Representação matricial de funções lineares.** Sejam V e W espaços vetoriais sobre $\mathbb{F}$. Uma função $f\colon V \to W$ é *linear* se

(L1) $f(\alpha\mathbf{v}) = \alpha f(\mathbf{v})$ para todo $\alpha \in \mathbb{F}$ e $\mathbf{v} \in V$ e

(L2) $f(\mathbf{v} + \mathbf{w}) = f(\mathbf{v}) + f(\mathbf{w})$ para todo $\mathbf{v}$ e $\mathbf{w}$ em V.

Observação. Vimos em §4.7 que se $A \in \mathbb{F}^{R\times C}$, então a função $f_A\colon \mathbf{v} \in \mathbb{F}^C \mapsto A\mathbf{v} \in \mathbb{F}^R$ é uma função linear.

Fato 4.8.1. *Seja* $f\colon V \to W$ *uma função linear. Então* $f(\mathbf{0}) = \mathbf{0}$*.*

Prova. Como $f(\mathbf{0}) = f(\mathbf{0} + \mathbf{0}) = f(\mathbf{0}) + f(\mathbf{0})$, segue que $f(\mathbf{0}) = \mathbf{0}$. □

Proposição 4.8.2. *Seja* $f\colon V \to W$ *uma função linear entre espaços vetoriais sobre* $\mathbb{F}$*. Então, para quaisquer* $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ *e* $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$*, temos*

$$f(\alpha_1\mathbf{v}_1 + \cdots + \alpha_n\mathbf{v}_n) = \alpha_1 f(\mathbf{v}_1) + \cdots + \alpha_n f(\mathbf{v}_n). \tag{23}$$

Prova. Indução em n (exercício). □

Seja $\mathbf{e}_s = \mathbb{1}_{\{s\}} \in \mathbb{F}^S$ para todo $s \in S$. Podemos escrever todo $\mathbf{v} \in \mathbb{F}^S$ em função desses $\mathbf{e}_s$:

$$\mathbf{v} = \sum_{s\in S} \mathbf{v}(s)\mathbf{e}_s. \tag{24}$$

Seja agora $f\colon \mathbb{F}^S \to \mathbb{F}^T$ uma função linear. Por (23) e (24), temos

$$f(\mathbf{v}) = \sum_{s\in S} \mathbf{v}(s) f(\mathbf{e}_s). \tag{25}$$

Seja $\mathbf{f}_t = \mathbb{1}_{\{t\}} \in \mathbb{F}^T$ para todo $t \in T$ e escreva cada $f(\mathbf{e}_s) \in \mathbb{F}^T$ em (25) em função desses $\mathbf{f}_t$:

$$f(\mathbf{e}_s) = \sum_{t\in T} A(t,s)\mathbf{f}_t. \tag{26}$$

Em vista de (25) e (26), temos

$$f(\mathbf{v}) = \sum_{s\in S} \mathbf{v}(s) f(\mathbf{e}_s) = \sum_{s\in S} \mathbf{v}(s) \sum_{t\in T} A(t,s)\mathbf{f}_t = \sum_{s\in S,\, t\in T} A(t,s)\mathbf{v}(s)\mathbf{f}_t. \tag{27}$$

A identidade (27) é equivalente a dizer que

$$f(\mathbf{v}) = A\mathbf{v}, \tag{28}$$

onde A é a matriz em $\mathbb{F}^{T\times S}$ tal que $(t,s) \mapsto A(t,s)$ para todo $(t,s) \in T \times S$. Provamos o seguinte fato.

Proposição 4.8.3. *Toda função linear* $f\colon \mathbb{F}^S \to \mathbb{F}^T$ *é tal que existe uma matriz* $A \in \mathbb{F}^{T\times S}$ *tal que* $f(\mathbf{v}) = A\mathbf{v}$ *para todo* $\mathbf{v} \in \mathbb{F}^S$*. De fato, tal matriz* A *é única e é tal que sua* s*-ésima coluna* A_{*s} *é* $f(\mathbf{e}_s)$ *para todo* $s \in S$*.*

A proposição acima tem o seguinte corolário. Denotemos por I_S a matriz identidade em $\mathbb{F}^{S\times S}$ e por $\mathrm{id}_{\mathbb{F}^S}$ a função identidade $\mathbb{F}^S \to \mathbb{F}^S$.

Corolário 4.8.4. *Seja* $A \in \mathbb{F}^{S\times S}$ *uma matriz e* $f_A\colon \mathbb{F}^S \to \mathbb{F}^S$ *a função linear* $\mathbf{v} \in \mathbb{F}^S \mapsto A\mathbf{v} \in \mathbb{F}^S$ *associada. Então* $A = I_S$ *se e só sem* $f_A = \mathrm{id}_{\mathbb{F}^S}$*.*

4.9. **Funções lineares: injeção e sobrejeção.** Seja $f\colon V \to W$ uma função linear. Definimos o *núcleo* $\operatorname{Ker} f$ de f como sendo a imagem inversa de $\{\mathbf{0}\}$:

$$\operatorname{Ker} f = f^{-1}(\{\mathbf{0}\}) = \{\mathbf{v} \in V\colon f(\mathbf{v}) = \mathbf{0}\}. \tag{29}$$

Se $f = f_A$ como em §4.7, isto é, f é a aplicação $\mathbf{v} \mapsto A\mathbf{v}$ para uma matriz A, então

$$\operatorname{Ker} f = \operatorname{Null} A. \tag{30}$$

Proposição 4.9.1. *Uma função linear $f\colon V \to W$ é injetora se e só se* $\operatorname{Ker} f = \{\mathbf{0}\}$.

No caso em que $f = f_A$ para uma matriz A, deduzimos que a aplicação $\mathbf{v} \mapsto A\mathbf{v}$ é injetora se e só se $\operatorname{Null} A = \{\mathbf{0}\}$. Na verdade, já conhecemos esse fato: isso segue do Teorema 3.5.5 (verifique).

O seguinte fato é simples mas importante.

Proposição 4.9.2. *Seja $f\colon V \to W$ uma função linear. A imagem* $\operatorname{Im} f$ *de f é um subespaço vetorial de W.*

Veremos mais adiante métodos para decidir se f é sobrejetora, isto é, se $\operatorname{Im} f = W$.

4.10. **Composição de funções lineares.** Sejam U, V e W espaços vetoriais sobre $\mathbb{F}$. Sejam $g\colon U \to V$ e $f\colon V \to W$ funções lineares. É imediato que a composta $h = f \circ g\colon U \to W$ é linear. Suponha agora que $U = \mathbb{F}^R$, $V = \mathbb{F}^S$ e $W = \mathbb{F}^T$. Nesse caso, sabemos da Proposição 4.8.3 que existem matrizes $A \in \mathbb{F}^{T\times S}$, $B \in \mathbb{F}^{S\times R}$ e $C \in \mathbb{F}^{T\times R}$ univocamente determinadas tais que $f(\mathbf{v}) = A\mathbf{v}$, $g(\mathbf{u}) = B\mathbf{u}$ e $h(\mathbf{u}) = C\mathbf{u}$, para todo $\mathbf{u} \in U$ e $\mathbf{v} \in V$.

Proposição 4.10.1. *Temos que $C = AB$.*

Prova. Pela Proposição 4.8.3, sabemos que, para todo $r \in R$, temos

$$C_{*r} = h(\mathbf{e}_r) \tag{31}$$

e

$$B_{*r} = g(\mathbf{e}_r). \tag{32}$$

Assim,

$$(AB)_{*r} = AB_{*r} = Ag(\mathbf{e}_r) = f(g(\mathbf{e}_r)) = (f \circ g)(\mathbf{e}_r) = h(\mathbf{e}_r) = C_{*r}. \tag{33}$$

onde a primeira igualdade vem da definição de produto de matrizes.

O resultado segue de (33). □

Usando a notação de §4.7, temos que $f = f_A$, $g = f_B$ e $h = f_C$. Lembrando que $h = f \circ g$, temos que $f_C = f_A \circ f_B$. A Proposição 4.10.1 acima diz que $f_C = f_{AB}$, donde temos que

$$f_A \circ f_B = f_{AB}. \tag{34}$$

Segue de (34) que $A(B\mathbf{u}) = f_A(f_B(\mathbf{u})) = (f_A \circ f_B)(\mathbf{u}) = f_{AB}(\mathbf{u}) = (AB)\mathbf{u}$ para todo $\mathbf{u} \in U$. Isto é,

$$A(B\mathbf{u}) = (AB)\mathbf{u} \tag{35}$$

para todo $\mathbf{u} \in U$. Na verdade, é um exercício simples provar (35) diretamente, a partir da definição de produto de matrizes (exercício).

Suponha agora que temos três matrizes A, B e C tais que os produtos $A(BC)$ e $(AB)C$ estejam bem definidos. Usando que $f_A \circ (f_B \circ f_C) = (f_A \circ f_B) \circ f_C$, a Proposição 4.10.1 implica que

$$A(BC) = (AB)C. \tag{36}$$

Isto é, a multiplicação de matrizes é associativa. Na verdade, supondo que $A \in \mathbb{F}^{P\times Q}$, $B \in \mathbb{F}^{Q\times R}$ e $C \in \mathbb{F}^{R\times S}$, é fácil ver diretamente que a (p, s)-ésima entrada das matrizes em (36) é

$$\sum_{q\in Q,\, r\in R} A(p, q)B(q, r)C(r, s). \tag{37}$$

4.11. **Inversão de matrizes.** Seja $A \in \mathbb{F}^{R\times C}$ uma matriz. Seja $f_A \colon \mathbb{F}^C \to \mathbb{F}^R$ a função linear associada a A (veja §4.7). Suponha que f_A seja inversível e seja $g = f_A^{-1}$.

Proposição 4.11.1. *A função $g = f_A^{-1} \colon \mathbb{F}^R \to \mathbb{F}^C$ é uma função linear.*

Prova. Exercício. □

Sabemos que toda função linear de $\mathbb{F}^R$ em $\mathbb{F}^C$ é da forma f_B para alguma matriz $B \in \mathbb{F}^{C\times R}$. Seja B tal que $g = f_A^{-1} = f_B$. Essa matriz B é a *inversa* de A. Denotamos a inversa de A por A^{-1}. Note que

$$f_A^{-1} = f_{A^{-1}}. \tag{38}$$

Note que definimos a inversa da matriz A somente no caso em que f_A é uma função inversível. É natural dizermos que A é *inversível* se f_A for inversível.

Proposição 4.11.2. *Sejam I_R a matriz identidade em $\mathbb{F}^{R\times R}$ e I_C a matriz identidade em $\mathbb{F}^{C\times C}$.*

(i) Seja $A \in \mathbb{F}^{R\times C}$ uma matriz inversível. Então $AA^{-1} = I_R$ e $A^{-1}A = I_C$.

(ii) Sejam $A \in \mathbb{F}^{R\times C}$ e $B \in \mathbb{F}^{C\times R}$ matrizes tais que $AB = I_R$ e $BA = I_C$. Então $B = A^{-1}$.

Prova. Exercício (veja (34) e Corolário 4.8.4). □

Proposição 4.11.3. *Sejam $A \in \mathbb{F}^{R\times C}$ e $B \in \mathbb{F}^{C\times D}$ matrizes inversíveis. Então o produto $AB \in \mathbb{F}^{R\times D}$ é inversível.*

Prova. Considere as funções $f_A \colon \mathbb{F}^C \to \mathbb{F}^R$ e $f_B \colon \mathbb{F}^D \to \mathbb{F}^C$ associadas a A e B. Como A e B são inversíveis, por definição f_A e f_B são funções inversíveis e $f_A^{-1} = f_{A^{-1}}$ e $f_B^{-1} = f_{B^{-1}}$. Basta agora verificar que $f_{B^{-1}A^{-1}} = f_{B^{-1}} \circ f_{A^{-1}}$ é a inversa da função f_{AB} (exercício). □

Observação. Seja $M \in \mathbb{F}^{R\times C}$ uma matriz. Por definição, M é inversível se e só se $f_M \colon \mathbb{F}^C \to \mathbb{F}^R$ é uma função inversível. Assim, é necessário que f_M seja injetora, que ocorre se e só se $\operatorname{Ker} f_M = \{\mathbf{0}\}$, isto é, $\operatorname{Null} M = \{\mathbf{0}\}$ (lembre-se da Proposição 4.9.1 e de (30)). Quando soubermos em que condições f_M é sobrejetora, teremos uma condição necessária e suficiente para M ser inversível.

§5. Bases

Sejam dados $\mathbf{a}_1, \ldots, \mathbf{a}_n \in \mathbb{F}^D$ e considere $V = \operatorname{Span}\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$. Se $\mathbf{v} \in V$, então existem $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ tais que

$$\mathbf{v} = \sum_{1\le i\le n} \alpha_i \mathbf{a}_i. \tag{39}$$

Naturalmente, o vetor dos coeficientes $\boldsymbol{\alpha} = [\alpha_1 \cdots \alpha_n]^\top \in \mathbb{F}^n$ é uma 'representação' de $\mathbf{v}$, no sentido que, se temos $\boldsymbol{\alpha}$, podemos recuperar $\mathbf{v}$ (basta usar (39)).

Observação. Veremos mais à frente que se os $\mathbf{a}_i$ $(1 \leq i \leq n)$ satisfizeram uma certa propriedade (forem 'linear independentes'), então o vetor dos coeficientes $\boldsymbol{\alpha}$ é univocamente definido.

Para termos tais representações $\boldsymbol{\alpha} = [\alpha_1 \cdots \alpha_n]^\top$ de $\mathbf{v} \in V$, naturalmente, precisamos dos vetores $\mathbf{a}_i$ $(1 \leq i \leq n)$ que geram V.

5.1. **Obtenção de geradores.** Seja $V \subset \mathbb{F}^D$ um espaço vetorial sobre $\mathbb{F}$. Queremos um conjunto gerador para V, isto é, um conjunto $S \subset V$ tal que $\operatorname{Span} S = V$. Podemos considerar dois procedimentos:

Algorithm 1: GROW

Entrada: Espaço vetorial $V \subset \mathbb{F}^D$ com D finito
Saída: $S \subset V$ finito tal que $V = \operatorname{Span} S$ e $|S|$ é mínimo

1 $S \leftarrow \emptyset$;
2 **while** $\operatorname{Span} S \neq V$ **do**
3 $\quad \mathbf{v} \leftarrow$ algum vetor em $V \setminus \operatorname{Span} S$;
4 $\quad S \leftarrow S \cup \{\mathbf{v}\}$;
5 **end**
6 **return** S;

Algorithm 2: SHRINK

Entrada: Espaço vetorial $V \subset \mathbb{F}^D$ com D finito
Saída: $S \subset V$ finito tal que $V = \operatorname{Span} S$ e $|S|$ é mínimo

1 $S \leftarrow$ algum S finito tal que $\operatorname{Span} S = V$;
2 **while** *existe* $\mathbf{v}$ *tal que* $\operatorname{Span}(S \setminus \{\mathbf{v}\}) = V$ **do**
3 $\quad S \leftarrow S \setminus \{\mathbf{v}\}$;
4 **end**
5 **return** S;

Observação. Note que, no momento, não sabemos se GROW necessariamente termina. Também não sabemos se existe um conjunto como especificado na linha 1 de SHRINK.

Veremos mais à frente que os dois procedimentos acima estão corretos: eles produzem conjuntos S como especificados. O seguinte resultado é fácil provar.

Proposição 5.1.1. *Valem as seguintes afirmações.*

(*i*) *Suponha que* GROW *termine com uma saída* S. *Então* $S \subset V$, S *é finito, e é tal que* $\operatorname{Span} S = V$.

(*ii*) *Suponha que a linha 1 de* SHRINK *seja executada com sucesso. Então* SHRINK *termina com* $S \subset V$ *finito tal que* $\operatorname{Span} S = V$.

Prova. Em GROW, o invariante $\operatorname{Span} S \subset V$ é mantido no laço. Isto é, toda vez que vamos executar o teste na linha 2, vale que $\operatorname{Span} S \subset V$ (exercício). Como GROW termina, a condição $\operatorname{Span} S \neq V$ na linha 2 falha, donde concluímos que $\operatorname{Span} S = V$ quando GROW termina.

Ademais, como GROW termina, temos que S é um conjunto finito. Claramente $S \subset V$. Isso prova (i).

Vamos agora provar (ii). Em SHRINK, o invariante $\operatorname{Span} S = V$ é mantido no laço da linha 2. Isto é, toda vez que vamos executar o teste na linha 2, vale que $\operatorname{Span} S = V$ (exercício). Claramente, o laço em SHRINK termina. Como o invariante $\operatorname{Span} S = V$ é mantido no laço, temos que $\operatorname{Span} S = V$ quando o laço termina, e assim o conjunto S devolvido por SHRINK é tal que $\operatorname{Span} S = V$. Claramente $S \subset V$ e S é finito. □

Observação. É importante perceber que ainda não sabemos por que GROW e SHRINK devolvem S de cardinalidade mínima.

5.1.1. *Espaço das arestas de um grafo.* Seja $G = (V, E)$ um grafo. O *espaço das arestas* $C_1(G)$ de G sobre $\mathrm{GF}(2)$ é o espaço vetorial sobre $\mathrm{GF}(2)$ gerado pelas funções características das arestas de G:

$$C_1(G) = \operatorname{Span}\{\mathbb{1}_e \colon e \in E\} \subset \mathrm{GF}(2)^V. \tag{40}$$

Podemos executar GROW e SHRINK para encontrar conjuntos geradores de cardinalidade mínima para $C_1(G)$. Para tanto, é importante entendermos quando

$$\mathbb{1}_e \in \operatorname{Span}\{\mathbb{1}_f \colon f \in F\}, \tag{41}$$

onde $e \in E$ e $F \subset E$.

Proposição 5.1.2. *Seja $G = (V, E)$ um grafo e sejam dados $e \in E$ e $F \subset E$. A condição (41) vale se e só se o grafo $H = (V, F)$ contém um (x, y)-caminho, onde $e = \{x, y\}$.*

Prova. Exercício. □

Dizemos que $F \subset E$ é *aresta-gerador* se toda aresta $e = \{x, y\}$ de G é tal que $H = (V, F)$ contém um (x, y)-caminho, isto é, existe um (x, y)-caminho que só usa arestas em F. A Proposição 5.1.2 implica que $F \subset E$ é aresta-gerador se e só se

$$C_1(G) = \operatorname{Span}\{\mathbb{1}_f \colon f \in F\}. \tag{42}$$

GROW e SHRINK tomam a seguinte forma quando especializados para encontrar conjuntos geradores de $C_1(G)$, isto é, conjuntos aresta-geradores de G.

Algorithm 3: GROWSF

Entrada: Grafo $G = (V, E)$ finito
Saída: $F \subset E$ aresta-gerador com $|F|$ é mínimo

1 $F \leftarrow \emptyset$;
2 **while** *existe* $e = \{x, y\} \in E$ *tal que não há* (x, y)*-caminho em* (V, F) **do**
3 $\quad F \leftarrow F \cup \{e\}$;
4 **end**
5 **return** F;

Algorithm 4: ShrinkSF

Entrada: Grafo $G = (V, E)$ finito

Saída: $F \subset E$ aresta-gerador com $|F|$ é mínimo

```
1 F ← E;
2 while existe f ∈ F tal que F \ {f} é aresta-gerador do
3 |   F ← F \ {f};
4 end
5 return F;
```

Observação. Ainda não sabemos por que GrowSF e ShrinkSF devolvem F de cardinalidade mínima.

5.2. **Dependência e independência linear.** Seja $V \subset \mathbb{F}^D$ um espaço vetorial sobre $\mathbb{F}$. Sejam dados $S \subset V$ e $\mathbf{v} \in S$. Dizemos que $\mathbf{v}$ é *supérfluo em* S se $\operatorname{Span}(S \setminus \{\mathbf{v}\}) = \operatorname{Span} S$.

Proposição 5.2.1. *São equivalentes*:

(*i*) $\mathbf{v}$ *é supérfluo em* S*;*

(*ii*) $\mathbf{v}$ *é uma combinação linear de vetores em* $S \setminus \{\mathbf{v}\}$*.*

Prova. Suponha que $\mathbf{v}$ seja supérfluo em S. Então $\mathbf{v} \in \operatorname{Span} S = \operatorname{Span}(S \setminus \{\mathbf{v}\})$, e portanto $\mathbf{v}$ é uma combinação linear de vetores em $S \setminus \{\mathbf{v}\}$. Suponha agora que $\mathbf{v}$ seja uma combinação linear de vetores em $S \setminus \{\mathbf{v}\}$. Precisamos provar que $\operatorname{Span} S \subset \operatorname{Span}(S \setminus \{\mathbf{v}\})$. Para tanto, seja $\mathbf{u} \in \operatorname{Span} S$. Então $\mathbf{u} = \sum_{1 \le i \le n} \alpha_i \mathbf{v}_i$ para alguns escalares α_i e vetores $\mathbf{v}_i \in S$ $(1 \le i \le n)$. Se nenhum dos $\mathbf{v}_i$ é $\mathbf{v}$, então $\mathbf{u} \in \operatorname{Span}\{\mathbf{v}_1, \dots, \mathbf{v}_n\} \subset \operatorname{Span}(S \setminus \{\mathbf{v}\})$. Suponha agora que $\mathbf{v}$ seja um dos $\mathbf{v}_i$. Sem perda de generalidade, suponha que $\mathbf{v} = \mathbf{v}_n$. Como estamos supondo que $\mathbf{v} = \sum_{1 \le j \le m} \beta_j \mathbf{w}_j$ para alguns escalares β_j e vetores $\mathbf{w}_j \in S \setminus \{\mathbf{v}\}$, o vetor $\mathbf{u}$ pode ser escrito como combinação linear dos vetores em $\{\mathbf{v}_i \colon 1 \le i < n\} \cup \{\mathbf{w}_j \colon 1 \le j \le m\} \subset S \setminus \{\mathbf{v}\}$. □

Note que no algoritmo Shrink, na linha 2, perguntamos se há $\mathbf{v} \in S$ que é supérfluo em S (e o removemos de S no corpo do laço nesse caso). Em Grow, procuramos $\mathbf{v}$ tal que $\mathbf{v}$ não seja supérfluo em $S \cup \{\mathbf{v}\}$ (e o adicionamos a S no corpo do laço nesse caso).

Sejam $\mathbf{v}_1, \dots, \mathbf{v}_n$ vetores em um espaço vetorial e $\alpha_1, \dots, \alpha_n$ escalares. A combinação linear

$$\alpha_1 \mathbf{v}_1 + \cdots + \alpha_n \mathbf{v}_n \tag{43}$$

é uma *combinação linear trivial* se os α_i são todos 0. A combinação linear (43) é *não-trivial* caso contrário. Naturalmente, uma combinação linear trivial tem valor $\mathbf{0}$. Pode acontecer de uma combinação linear não-trivial ter valor $\mathbf{0}$:

$$\alpha_1 \mathbf{v}_1 + \cdots + \alpha_n \mathbf{v}_n = \mathbf{0} \tag{44}$$

com os α_i não todos nulos. Nesse caso, dizemos que $\mathbf{0}$ é uma combinação linear não-trivial dos $\mathbf{v}_i$ $(1 \le i \le n)$.

Proposição 5.2.2. *São equivalentes*:

(*i*) S *contém um vetor supérfluo;*

(*ii*) $\mathbf{0}$ *é uma combinação linear não-trivial de elementos de* S*.*

Prova. Exercício. □

Definição 5.2.3 (Independência linear; dependência linear). Dizemos que um conjunto S de vetores é *linearmente independente* se toda combinação linear não-trivial de vetores de S é não nulo. Caso contrário, S é *linearmente dependente*.

Proposição 5.2.4. *Seja $S \subset V$ um conjunto de vetores. São equivalentes*:

(*i*) *S é linearmente independente;*

(*ii*) *S não contém elementos supérfluos;*

(*iii*) *se vale (44) para escalares α_i e $\mathbf{v}_i \in S$ $(1 \leq i \leq n)$, então todos os α_i são nulos.*

Prova. Exercício. □

Observação. É comum provar que um conjunto de vetores é linearmente independente verificando a asserção (*iii*) da Proposição 5.2.4.

5.2.1. *Arestas linearmente independentes em um grafo.* Seja $G = (V, E)$ um grafo e seja $C_1(G) = \mathrm{Span}\{\mathbb{1}_e \colon e \in E\}$ o espaço das arestas de G (veja §5.1.1). Definimos um conjunto de arestas $F \subset E$ como sendo *linearmente independente* se $\{\mathbb{1}_f \colon f \in F\} \subset C_1(G)$ for linearmente independente. Dizemos que $F \subset E$ é *acíclico* se não há um circuito em G que tem todas suas arestas em F.

Proposição 5.2.5. *Um conjunto de arestas $F \subset E$ é linearmente independente se e só se F é acíclico.*

Prova. Exercício. □

5.3. **Hereditariedade de independência linear.** A propriedade de ser linearmente independente é uma propriedade *hereditária*, isto é, vale a afirmação a seguir.

Proposição 5.3.1. *Seja S um conjunto linearmente independente de vetores e seja $T \subset S$. Então T é linearmente independente.*

Prova. Se vale a afirmação em Proposição 5.2.4(*iii*) para S, então ela também vale para T. □

5.4. **Análise dos algoritmos** Grow **e** Shrink**.** Vamos verificar que os conjuntos devolvidos por Grow e Shrink são conjuntos independentes.

Proposição 5.4.1. *Suponha que* Grow *devolve o conjunto S. Então S é um conjunto linearmente independente.*

Prova. Suponha que Grow adiciona a S os vetores $\mathbf{v}_1, \ldots, \mathbf{v}_n$, nessa ordem. Provamos que esses n vetores são linearmente independentes por indução em n. A afirmação é válida para $n = 0$. Suponha agora que n seja positivo e que a afirmação seja válida para valores menores de n. Se os $\mathbf{v}_i$ $(1 \leq i \leq n)$ não são linearmente independentes, então há escalares α_i $(1 \leq i \leq n)$ não todos nulos tais que (44) vale. Pela hipótese de indução, $\mathbf{v}_i$ $(1 \leq i < n)$ são linearmente independentes. Assim, temos $\alpha_n \neq 0$ (por que?). Dividindo (44) por α_n e rearranjando, obtemos

$$\mathbf{v}_n = -\alpha_n^{-1}\alpha_1\mathbf{v}_1 - \cdots - \alpha_n^{-1}\alpha_{n-1}\mathbf{v}_{n-1}. \tag{45}$$

Segue que $\mathbf{v}_n \in \mathrm{Span}\{\mathbf{v}_1, \ldots, \mathbf{v}_{n-1}\}$, contradizendo a condição na linha 3 de Grow para a escolha de $\mathbf{v}_n$. □

Proposição 5.4.2. *Suponha que* Shrink *devolve o conjunto S. Então S é um conjunto independente.*

Prova. Note que o laço de Shrink remove vetores supérfluos de S e que o laço termina quando não há mais vetores supérfluos em S. Assim, o conjunto S devolvido por Shrink satisfaz a afirmação (*ii*) da Proposição 5.2.4. O resultado segue. □

As Proposições 5.1.1, 5.4.1 e 5.4.2 implicam que os conjuntos S devolvidos por Grow e Shrink geram V, isto é, $\operatorname{Span} S = V$, e são linearmente independentes. Tais conjuntos são chamados de "bases" de V.

5.5. **Bases de espaços vetoriais.** A seguinte definição é muito importante.

Definição 5.5.1 (Base). Seja V um espaço vetorial. Um conjunto S de vetores de V é uma *base* de V se

(B1) S gera V, isto é, $\operatorname{Span} S = V$ e
(B2) S é linearmente independente.

Exemplo 5.5.2. Seja $G = (V, E)$ um grafo. O conjunto $\{\mathbb{1}_f : f \in F\}$ é uma base de $C_1(G)$ se e só se (a) F é aresta-gerador e (b) F é acíclico. (Exercício: prove essa asserção.) Tais conjuntos F são chamados de *florestas aresta-geradoras*.

Já observamos que se o algoritmo Grow termina, então ele devolve uma base da entrada V. Observamos também que se a linha 1 de Shrink pode ser executada, então Shrink devolve uma base da entrada V. Assim, para obtermos uma base de um espaço vetorial V, basta provar que Grow com entrada V termina, ou que a linha 1 de Shrink pode ser executada com a entrada V.

Exemplo 5.5.3. Seja $G = (V, E)$ um grafo. Os algoritmos GrowSF e ShrinkSF executados com entrada G terminam e devolvem uma floresta aresta-geradora.

Seja V um espaço vetorial, B uma base de V e $\mathbf{v}$ um elemento de V. Pelo fato de B gerar V, há escalares $\alpha_{\mathbf{b}}$ ($\mathbf{b} \in B$) tais que

$$\mathbf{v} = \sum_{\mathbf{b} \in B} \alpha_{\mathbf{b}} \mathbf{b}, \tag{46}$$

isto é, podemos "escrever $\mathbf{v}$ na base B". O seguinte fato implica que há exatamente uma forma de se escrever $\mathbf{v}$ na base B.

Proposição 5.5.4. *Seja S um conjunto de vetores linearmente independentes e suponha que*

$$\mathbf{v} = \sum_{1 \le i \le m} \alpha_i \mathbf{v}_i, \tag{47}$$

onde os $\mathbf{v}_i$ são elementos distintos de S e os α_i são todos não-nulos. Suponha também que

$$\mathbf{v} = \sum_{1 \le j \le n} \beta_j \mathbf{u}_j. \tag{48}$$

onde os $\mathbf{u}_j$ são elementos distintos de S e os β_j são todos não-nulos. Então

(*i*) $\{\mathbf{v}_i : 1 \le i \le m\} = \{\mathbf{u}_j : 1 \le j \le n\}$, *de forma que $m = n$ e existe uma bijeção $\sigma : [m] = \{1, \dots, m\} \to [m]$ tal que $\mathbf{u}_j = \mathbf{v}_{\sigma(j)}$ para todo $1 \le j \le n = m$ e*
(*ii*) $\beta_j = \alpha_{\sigma(j)}$ *para todo $1 \le j \le n = m$.*

Prova. Segue do fato que $\beta_1 \neq 0$ e que

$$\sum_{1\leq i\leq m} \alpha_i \mathbf{v}_i = \sum_{1\leq j\leq n} \beta_j \mathbf{u}_j \tag{49}$$

que $\mathbf{u}_1 \in \mathrm{Span}\{\mathbf{v}_1, \ldots, \mathbf{v}_m, \mathbf{u}_2, \ldots, \mathbf{u}_n\}$. Segue que $\mathbf{u}_1$ é igual a algum dos $\mathbf{v}_i$ (por quê?). Este argumento mostra que de fato $\{\mathbf{v}_i \colon 1 \leq i \leq m\} = \{\mathbf{u}_j \colon 1 \leq j \leq n\}$. Segue que $m = n$ e que existe a bijeção $\sigma \colon [m] \to [m]$ como especificado em (*i*). A identidade (49) toma a forma

$$\sum_{1\leq i\leq m} \alpha_i \mathbf{v}_i = \sum_{1\leq j\leq m} \beta_j \mathbf{v}_{\sigma(j)} = \sum_{1\leq i\leq m} \beta_{\sigma^{-1}(i)} \mathbf{v}_i. \tag{50}$$

Rearranjando,

$$\sum_{1\leq i\leq m} (\alpha_i - \beta_{\sigma^{-1}(i)})\mathbf{v}_i = \mathbf{0}. \tag{51}$$

Pela independência linear dos $\mathbf{v}_i$, temos que $\alpha_i = \beta_{\sigma^{-1}(i)}$ para todo i. Segue que $\alpha_{\sigma(j)} = \beta_j$ para todo j. □

A proposição abaixo sobre grafos é uma consequência da unicidade da representação de vetores em uma dada base.

Proposição 5.5.5. *Seja $G = (V, E)$ um grafo. Sejam $F \subset E$ uma floresta aresta-geradora de G e x e y vértices de G tais que existe um (x, y)-caminho em G. Então existe exatamente um (x, y)-caminho em G que usa apenas arestas em F.*

Prova. Exercício. □

5.5.1. *Representação em bases e mudança de base.* Seja $V \subset \mathbb{F}^D$ um espaço vetorial, B uma base de V e $\mathbf{v}$ um elemento de V. Lembre que podemos escrever $\mathbf{v}$ na base B:

$$\mathbf{v} = \sum_{\mathbf{b}\in B} \alpha_{\mathbf{b}} \mathbf{b}, \tag{52}$$

onde os escalares $\alpha_{\mathbf{b}}$ ($\mathbf{b} \in B$) estão univocamente definidos. Podemos montar o vetor de coeficientes $\boldsymbol{\alpha} = [\alpha_{\mathbf{b}} \colon \mathbf{b} \in B] \in \mathbb{F}^B$ e pensar que $\boldsymbol{\alpha} \in \mathbb{F}^B$ representa $\mathbf{v}$. Note que encontrar $\boldsymbol{\alpha}$ dado $\mathbf{v}$ equivale a resolver a equação

$$M\mathbf{x} = \mathbf{v}, \tag{53}$$

onde $M \in \mathbb{F}^{D\times B}$ é tal que sua $\mathbf{b}$-ésima coluna é $\mathbf{b}$ ($\mathbf{b} \in B$). Intuitivamente, se $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$, então

$$M = \left[\mathbf{b}_1 \,\middle|\, \ldots \,\middle|\, \mathbf{b}_m\right]. \tag{54}$$

Note também que a função linear $f_M \colon \mathbb{F}^B \to V$ que leva $\mathbf{x} \in \mathbb{F}^B$ em $M\mathbf{x} \in V$ é bijetora (por quê?).

Consideramos agora o *problema de mudança de base*: se temos a representação $\boldsymbol{\alpha} \in \mathbb{F}^B$ de $\mathbf{v}$ na base B como acima e B' é outra base de V, como podemos obter a representação $\boldsymbol{\alpha}' \in \mathbb{F}^{B'}$ de $\mathbf{v}$ na base B'? Gostaríamos de obter $\boldsymbol{\alpha}'$ de alguma forma simples a partir de $\boldsymbol{\alpha}$.

Considere a matriz $M' \in \mathbb{F}^{D\times B'}$ tal que sua $\mathbf{b}'$-ésima coluna é $\mathbf{b}'$ ($\mathbf{b}' \in B'$). Intuitivamente, se $B' = \{\mathbf{b}'_1, \ldots, \mathbf{b}'_{m'}\}$, então

$$M' = \left[\mathbf{b}'_1 \,\middle|\, \ldots \,\middle|\, \mathbf{b}'_{m'}\right]. \tag{55}$$

Considere a função linear $f_{M'}\colon \mathbb{F}^{B'} \to V$, que leva $\mathbf{x} \in \mathbb{F}^{B'}$ em $M'\mathbf{x} \in V$. Lembre que $f_{M'}$ é bijetora, e assim é inversível. Basta agora observar que

$$\boldsymbol{\alpha}' = (f_{M'}^{-1} \circ f_M)(\boldsymbol{\alpha}) = f_{(M')^{-1}M}(\boldsymbol{\alpha}) = (M')^{-1}M\boldsymbol{\alpha}. \tag{56}$$

5.5.2. *O caso dos espaços vetoriais finitos sobre* GF(2). Seja V um espaço vetorial sobre GF(2) finito, isto é, com $|V|$ finito. O algoritmo Shrink encontra uma base para V, digamos B. A Proposição 5.5.4 implica que se B tem n elementos, então $|V| = 2^n$ (exercício). Em particular, se B' for outra base de V, então B' também tem n elementos. Esse valor comum n é a *dimensão* de V.

Novamente usando o fato que V é finito, podemos concluir que o algoritmo Grow termina com entrada V. Ademais, como Grow devolve uma base de V, vemos que a saída de Grow sempre tem n elementos.

Note que, no caso de espaços vetoriais finitos sobre GF(2), deduzimos que Grow e Shrink funcionam como prometido: eles devolvem conjuntos geradores de cardinalidade mínima, a saber, com dimensão de V elementos.

Proposição 5.5.6. *Seja V um espaço vetorial sobre* GF(2) *finito. Valem as seguintes afirmações.*

(*i*) Shrink *e* Grow *devolvem bases de V.*

(*ii*) *Todas as bases de V têm a mesma cardinalidade.*

(*iii*) *A cardinalidade comum n das bases de V é tal que $|V| = 2^n$.*

Seja V como na proposição acima. Vamos denotar a dimensão n de V por $\dim V$.

Corolário 5.5.7. *Seja V um espaço vetorial finito sobre* GF(2). *Se S é um conjunto com mais de $\dim V$ vetores, então S não é linearmente independente.*

Prova. Seja $n = \dim V$. Temos que $|V| = 2^n$. Se temos mais de n vetores em S, então, pelo princípio da casa dos pombos, há duas combinações lineares de vetores de S que tem o mesmo valor. Isto é, há S_1 e S_2 subconjuntos distintos de S tais que $\sum_{\mathbf{s}\in S_1} \mathbf{s} = \sum_{\mathbf{s}\in S_2} \mathbf{s}$. Segue que $\sum_{\mathbf{s}\in S_1 \triangle S_2} \mathbf{s} = \mathbf{0}$ é uma dependência linear de vetores em S. □

Vários dos fatos que pudemos deduzir nessa seção sobre espaços vetoriais finitos sobre GF(2) serão provados em situações gerais mais à frente.

5.6. **Propriedades de troca de conjuntos geradores.** Descrevemos agora duas propriedades que conjuntos geradores satisfazem.

Proposição 5.6.1. *Sejam V um espaço vetorial e $A \subset V$. Suponha que $\mathbf{b} \in (\operatorname{Span} A) \setminus A$ seja um vetor não-nulo. Então existe $\mathbf{a} \in A$ tal que $(A \setminus \{\mathbf{a}\}) \cup \{\mathbf{b}\}$ gera* Span A.

Prova. Escreva $\mathbf{b}$ como combinação linear de elementos de A. Como $\mathbf{b} \neq \mathbf{0}$, tal combinação linear é não-trivial. Suponha que $\mathbf{a} \in A$ ocorre nessa combinação linear com coeficiente não-nulo. Então $\mathbf{a} \in \operatorname{Span}\big((A \setminus \{\mathbf{a}\}) \cup \{\mathbf{b}\}\big)$. Isso implica que $(A \setminus \{\mathbf{a}\}) \cup \{\mathbf{b}\}$ gera Span A (exercício). □

Na proposição acima, não temos "controle" sobre qual $\mathbf{a}$ é removido de A. A proposição a seguir dá certo controle sobre esse elemento.

Proposição 5.6.2. *Sejam V um espaço vetorial e $A \subset V$. Suponha que $A' \subset A$ e $\mathbf{b} \in (\operatorname{Span} A) \setminus A$ são tais que $A' \cup \{\mathbf{b}\}$ é linearmente independente. Então existe $\mathbf{a} \in A \setminus A'$ tal que $(A \setminus \{\mathbf{a}\}) \cup \{\mathbf{b}\}$ gera* Span A.

Prova. Escreva $\mathbf{b}$ como combinação linear de elementos de A. Como $A' \cup \{\mathbf{b}\}$ é linearmente independente, algum $\mathbf{a} \in A \setminus A'$ ocorre nessa combinação linear com coeficiente não-nulo (por quê?). Segue que $\mathbf{a} \in \operatorname{Span}\big((A \setminus \{\mathbf{a}\}) \cup \{\mathbf{b}\}\big)$, e a prova segue como na prova da Proposição 5.6.1. □

Podemos usar a Proposição 5.6.2 para provar que um algoritmo guloso resolve o *problema do conjunto gerador de peso mínimo*. Neste problema, recebemos um conjunto X de vetores de algum espaço vetorial V. Recebemos também uma função $w\colon X \to \mathbb{R}$ que atribui *peso* $w(\mathbf{x})$ a cada $\mathbf{x} \in X$. O objetivo é encontrar um subconjunto S de X de peso mínimo tal que $\operatorname{Span} S = \operatorname{Span} X$. Aqui, o peso $w(S)$ de S é simplesmente $\sum_{\mathbf{s}\in S} w(\mathbf{s})$.

O algoritmo Guloso resolve esse problema.

Algorithm 5: Guloso

Entrada: $X \subset V$ finito e $w\colon X \to \mathbb{R}$

Saída: $S \subset X$ tal que $\operatorname{Span} S = \operatorname{Span} X$ e $w(S)$ é mínimo

```
1 Sejam x_1, ..., x_n os vetores em X em ordem não-decrescente de peso: isto é,
    w(x_1) ≤ ··· ≤ w(x_n);
2 S ← ∅;
3 for i = 1, ..., n do
4 |   if x_i ∉ Span S then
5 |   |   S ← S ∪ {x_i};
6 |   end
7 end
8 return S;
```

Teorema 5.6.3. *O algoritmo* Guloso *resolve o problema do conjunto gerador de peso mínimo.*

Prova. Seja S o conjunto devolvido por Guloso. Um argumento simples mostra que $\operatorname{Span} S = \operatorname{Span} X$ (exercício). Seja S^* um conjunto gerador de $\operatorname{Span} X$ de peso mínimo. Se $S = S^*$ então Guloso funcionou corretamente. Suponha por contradição que $S \neq S^*$ e seja i o menor índice tal que $\mathbf{x}_i \in S^* \triangle S = (S^* \setminus S) \cup (S \setminus S^*)$. Dentre todas as possíveis escolhas de S^*, escolha uma que maximiza o valor de i. Vamos derivar uma contradição construindo outra solução S^{**} com tal índice i maior.

Observemos inicialmente que S^* é um conjunto linearmente independente (por quê?). Também é verdade que S é um conjunto linearmente independente (exercício). Sejam $S_{<i} \subset S$ e $S^*_{<i} \subset S^*$ dados por

$$S_{<i} = \{\mathbf{x}_j \in S\colon j < i\} \tag{57}$$

e

$$S^*_{<i} = \{\mathbf{x}_j \in S^*\colon j < i\}. \tag{58}$$

Pela definição de i, temos que $S_{<i} = S^*_{<i}$. Como $S_{<i} \cup \{\mathbf{x}_i\} = S^*_{<i} \cup \{\mathbf{x}_i\}$ está contido ou em S ou em S^* e tanto S como S^* são linearmente independentes, segue que $\mathbf{x}_i \notin \operatorname{Span} S_{<i}$. Segue que $\mathbf{x}_i$ é adicionado a S na linha 5 de Guloso. Deduzimos que $\mathbf{x}_i \notin S^*$. Aplicamos agora a Proposição 5.6.2, tomando $A = S^*$, $A' = S^*_{<i}$ e $\mathbf{b} = \mathbf{x}_i$. Note que tal escolha faz com que as hipóteses daquela proposição sejam satisfeitas (exercício). Segue que existe $\mathbf{x}_k$ com $k > i$ tal

que, tomando $S^{**} = (S^* \setminus \{\mathbf{x}_k\}) \cup \{\mathbf{x}_i\}$, temos que (a) S^{**} gera $\operatorname{Span} X$ e $(\mathbf{b})$ $w(S^{**}) \leq w(S^*)$. Podemos concluir que S^{**} é um conjunto gerador de $\operatorname{Span} X$ de peso mínimo. Basta agora observar que o menor índice dos elementos em $S^{**} \triangle S$ é maior que i, e isso contradiz a escolha de S^*. □

Podemos especializar Guloso para resolver o *problema da floresta aresta-geradora de peso mínimo* (mais conhecido como o *problema da árvore geradora mínima*). Neste problema, recebemos um grafo $G = (V, E)$ e uma função $w\colon E \to \mathbb{R}$ que atribui *peso* $w(e)$ a cada $e \in E$. O objetivo é encontrar um subconjunto F de E de peso mínimo tal que F seja aresta-geradora em G, isto é, tal que, para toda aresta $e = \{x, y\}$ de G, há um (x, y)-caminho em G que usa somente arestas em F. Aqui, o peso $w(F)$ de F é simplesmente $\sum_{f \in F} w(f)$.

O algoritmo Kruskal, que é uma especialização de Guloso, resolve esse problema.

Algorithm 6: Kruskal

Entrada: $G = (V, E)$ grafo e $w\colon E \to \mathbb{R}$

Saída: $F \subset E$ tal que F é aresta-gerador e $w(F)$ é mínimo

```
1 Sejam e_1, ..., e_m as arestas de G em ordem não-decrescente de peso: isto é,
    w(e_1) ≤ ··· ≤ w(e_m);
2 F ← ∅;
3 for i = 1, ..., m do
4 |   if não existe (x, y)-caminho em (V, F) onde e_i = {x, y} then
5 |   |   F ← F ∪ {e_i};
6 |   end
7 end
8 return F;
```

Teorema 5.6.4. *O algoritmo* Kruskal *resolve o problema da floresta aresta-geradora de peso mínimo.*

Prova. Exercício. □

Os algoritmos Guloso e Kruskal são versões de Grow. Os algoritmos Mesquinho e Kruskal invertido são as versões correspondentes a Shrink. A prova da correção de Mesquinho e Kruskal invertido fica como exercício.

Algorithm 7: MESQUINHO

Entrada: $X \subset V$ finito e $w\colon X \to \mathbb{R}$

Saída: $S \subset X$ tal que $\operatorname{Span} S = \operatorname{Span} X$ e $w(S)$ é mínimo

Sejam $\mathbf{x}_1, \dots, \mathbf{x}_n$ os vetores em X em ordem não-decrescente de peso: isto é, $w(\mathbf{x}_1) \leq \cdots \leq w(\mathbf{x}_n)$;
$S \leftarrow X$;
for $i = n, \dots, 1$ **do**
  if $\mathbf{x}_i \in \operatorname{Span}(S \setminus \{\mathbf{x}_i\})$ **then**
    $S \leftarrow S \setminus \{\mathbf{x}_i\}$;
  end
end
return S;

Algorithm 8: KRUSKAL INVERTIDO

Entrada: $G = (V, E)$ grafo e $w\colon E \to \mathbb{R}$

Saída: $F \subset E$ tal que F é aresta-gerador e $w(F)$ é mínimo

Sejam $e_1, \dots, e_m$ as arestas de G em ordem não-decrescente de peso: isto é, $w(e_1) \leq \cdots \leq w(e_m)$;
$F \leftarrow E$;
for $i = m, \dots, 1$ **do**
  if *existe* (x, y)*-caminho em* $(V, F \setminus \{e_i\})$ *onde* $e_i = \{x, y\}$ **then**
    $F \leftarrow F \setminus \{e_i\}$;
  end
end
return F;

§6. DIMENSÃO

Em §5.5.2, vimos que há uma noção bem definida de 'dimensão' no caso de espaços vetoriais sobre GF(2) finitos: tais espaços vetoriais V são tais que todas as suas bases tem um mesmo número de elementos, e denominamos esse número de *dimensão* de V. Veremos agora que podemos definir dimensão para espaços quaisquer.

6.1. **Dimensão de espaços vetoriais.** Começamos com a seguinte proposição.

Proposição 6.1.1. *Seja S um conjunto de vetores em um espaço vetorial V. Suponha que $T \subset \operatorname{Span} S$ seja um conjunto linearmente independente. Então $|T| \leq |S|$.*

Prova. A prova é baseada na Proposição 5.6.2 e pode ser formulada de forma algorítmica. Considere o algoritmo MORPH. Verifique que MORPH de fato devolve S' como especificado. Como $T \subset S'$ e $|S'| = |S|$, vale que $|T| \leq |S|$. □

Podemos deduzir do algoritmo MORPH usado na prova da Proposição 6.1.1 o seguinte resultado mais refinado.

Algorithm 9: MORPH

Entrada: $S \subset V$ e $T \subset \operatorname{Span} S$ linearmente independente, onde V é um espaço vetorial
Saída: $S' \subset V$ tal que $|S'| = |S|$, $T \subset S'$ e $\operatorname{Span} S' = \operatorname{Span} S$

Suponha $T = \{\mathbf{v}_1, \dots, \mathbf{v}_t\}$;
$S' \leftarrow S$; $A \leftarrow \emptyset$;
for $i = 1, \dots, t$ **do**
  /* $A \cup \{\mathbf{v}_i\} = \{\mathbf{v}_1, \dots, \mathbf{v}_i\}$ e assim $A \cup \{\mathbf{v}_i\}$ é linearmente independente. Ademais, vale que $\operatorname{Span} S' = \operatorname{Span} S$. */
  if $\mathbf{v}_i \in S'$ **then**
    $A \leftarrow A \cup \{\mathbf{v}_i\}$;
    continue;
  end
  /* Como $\mathbf{v}_i \in T \setminus S' \subset (\operatorname{Span} S) \setminus S' = (\operatorname{Span} S') \setminus S'$, segue da Proposição 5.6.2 que existe $\mathbf{w} \in S' \setminus A$ como abaixo. */
  Seja $\mathbf{w} \in S' \setminus A$ tal que $\operatorname{Span}\big((S' \setminus \{\mathbf{w}\}) \cup \{\mathbf{v}_i\}\big) = \operatorname{Span} S'$;
  $S' \leftarrow (S' \setminus \{\mathbf{w}\}) \cup \{\mathbf{v}_i\}$;
  $A \leftarrow A \cup \{\mathbf{v}_i\}$;
end
return S';

Lema 6.1.2 (Lema de substituição de Steinitz)**.** *Seja S um conjunto de vetores em um espaço vetorial V. Suponha que $T \subset \operatorname{Span} S$ seja um conjunto finito linearmente independente. Então existe $S_1 \subset S$ tal que*

(*i*) $|T \cup S_1| = |S|$
(*ii*) $\operatorname{Span}(T \cup S_1) = \operatorname{Span} S$.

Prova. Segue do algoritmo MORPH: a saída S' de MORPH é da forma $T \cup S_1$ onde $S = S_0 \cup S_1$ e $|S_0| = |T|$. O algoritmo MORPH iterativamente substitui os elementos de S_0 por elementos de T. □

Teorema 6.1.3. *Seja V um espaço vetorial e suponha que*

$$n = \min\{|S| \colon S \subset V \text{ tal que } \operatorname{Span} S = V\} \tag{59}$$

seja finito. Fixe $B \subset V$. Quaisquer duas das afirmações abaixo implica a terceira:

(*i*) $V = \operatorname{Span} B$;
(*ii*) B *é linearmente independente;*
(*iii*) $|B| = n$.

Prova. Fixemos inicialmente $S \subset V$ tal que $\operatorname{Span} S = V$ e $|S| = n$. Suponha que agora que valham (*i*) e (*ii*). Vamos provar que (*iii*) vale. Pela Proposição 6.1.1, segue que $|B| \leq |S| = n$. Pela definição de n, como $\operatorname{Span} B = V$, segue que $|B| \geq n$ e portanto $|B| = n$. Suponha agora que valem (*i*) e (*iii*). Provemos que (*ii*) vale. Suponha que B não seja linearmente independente. Então, pela Proposição 5.2.4, há um vetor supérfluo $\mathbf{v}$ em B. Considere $B' = B \setminus \{\mathbf{v}\}$. Temos que $\operatorname{Span} B' = \operatorname{Span} B = V$. Entretanto, $|B'| = |B| - 1 = n - 1$, o que contradiz a definição de n. Essa contradição prova que B é necessariamente linearmente independente, isto é, que (*ii*) vale. Finalmente, suponha que (*ii*) e (*iii*) valham. Provemos que (*i*) também vale. Suponha por contradição que $\operatorname{Span} B \neq V$ e seja $\mathbf{v} \in V \setminus \operatorname{Span} B$. Segue que $B' = B \cup \{\mathbf{v}\}$ é linearmente

independente. Lembre que fixamos $S \subset V$ tal que $\operatorname{Span} S = V$ e $|S| = n$. Pela Proposição 6.1.1, temos que $n + 1 = |B'| \leq |S| = n$. Esta contradição mostra que $\operatorname{Span} B = V$. □

Note que se (i) e (ii) valem, então B é uma base de V. Assim, o teorema acima implica que toda base de V tem n elementos, onde n é como definido em (59). Em particular, todas as bases de V têm o mesmo número de elementos. O teorema acima também diz duas outras coisas: (1) se $\operatorname{Span} B = V$ e $|B| = n$, então B é uma base e (2) se B é linearmente independente e $|B| = n$, então B é uma base de V.

Definição 6.1.4 (Dimensão de um espaço vetorial; $\dim V$). Seja V um espaço vetorial com

$$n = \min\{|S| \colon S \subset V \text{ tal que } \operatorname{Span} S = V\} \tag{60}$$

finito. Definimos a dimensão $\dim V$ de V como sendo o inteiro n em (60). Se um espaço vetorial V é tal que $\operatorname{Span} S \neq V$ para qualquer V finito, dizemos que V tem dimensão infinita.

Devido ao Teorema 6.1.3, $\dim V$ é também a cardinalidade comum das bases de V.

Proposição 6.1.5. *Seja D um conjunto finito. Então $\mathbb{F}^D$ tem dimensão $|D|$.*

Prova. Seja $B = \{\mathbb{1}_{\{d\}} \in \mathbb{F}^D \colon d \in D\}$. Como D é finito, temos que $\operatorname{Span} B = \mathbb{F}^D$. Claramente, os vetores em B são linearmente independentes. Assim, B é uma base de $\mathbb{F}^D$, donde $\dim \mathbb{F}^D = |B| = |D|$. □

Proposição 6.1.6. *Sejam $\mathbf{v}_1, \ldots, \mathbf{v}_N$ vetores em um espaço vetorial V de dimensão n. Se $N > n$, então $\mathbf{v}_1, \ldots, \mathbf{v}_N$ não podem ser linearmente independentes.*

Prova. Seja B uma base de V, de forma que $|B| = \dim V = n$. Se os vetores $\mathbf{v}_i$ $(1 \leq i \leq N)$ fossem linearmente independentes, então a Proposição 6.1.1 implicaria que $N \leq n$. Assim, os $\mathbf{v}_i$ $(1 \leq i \leq N)$ não são linearmente independentes. □

6.2. **Alguns fatos sobre dimensão.** Os seguintes fatos são úteis.

Proposição 6.2.1. *Seja V um espaço vetorial sobre $\mathbb{F}$ e seja $S \subset V$ um conjunto finito. Então existe $T \subset S$ tal que T é base de $\operatorname{Span} S$. Em particular, $\dim \operatorname{Span} S = |T| \leq |S|$.*

Prova. Seja $T \subset S$ com $\operatorname{Span} T = \operatorname{Span} S$ e minimal com essa propriedade (isto é, tal que se $T' \subset T$ e $T' \neq T$, então $\operatorname{Span} T' \neq \operatorname{Span} S$). A existência de tal T segue do fato que S é finito. Então T é linearmente independente (exercício). Assim, T é base de $\operatorname{Span} S$. □

A seguinte proposição afirma que todo conjunto linearmente independente de vetores em um espaço vetorial pode ser estendido a uma base do espaço. Em particular, todo espaço vetorial tem uma base.

Proposição 6.2.2. *Seja $V \subset \mathbb{F}^D$ um espaço vetorial sobre $\mathbb{F}$ com D finito, e seja $S \subset V$ um conjunto linearmente independente. Então existe uma base B de V com $S \subset B$.*

Prova. Considere um conjunto $B \subset V$ que contém S linearmente independente e maximal com essa propriedade (isto é, tal que se $B \subset B'$ e $B \neq B'$, então B' não é linearmente independente). A existência de tal B segue do fato que D é finito: se tivéssemos uma sequência $S = B_0 \subset B_1 \subset B_2 \subset \ldots$ de conjuntos linearmente independentes estritamente crescente, então teríamos um conjunto com mais de $|D|$ vetores linearmente independentes em $\mathbb{F}^D$, mas isso é impossível,

pois quaisquer $|D|$ deles formam uma base (Teorema 6.1.3). Confirmamos assim que B como especificado existe. Afirmamos que B é uma base de V. Basta verificar que $\operatorname{Span} B = V$. Claramente $\operatorname{Span} B \subset V$. Suponha que $\operatorname{Span} B \neq V$. Tome $\mathbf{v} \in V \setminus \operatorname{Span} B$. Temos que $B' = B \cup \{\mathbf{v}\} \subset V$ é linearmente independente e $B' \neq B$. Tal B' contradiz a maximalidade de B. Segue que $\operatorname{Span} B = V$. □

Observação. É fácil verificar que qualquer $B \subset V$ linearmente independente maximal é base de V. Quando V tem dimensão finita, a existência de tal B é simples de provar (como vimos acima). No caso em que V tem dimensão infinita, esse fato vale, mas a prova é mais sutil. A conclusão é que todo espaço vetorial tem uma base.

Proposição 6.2.3. *Seja U um subespaço vetorial de um espaço V com V de dimensão finita. Valem as seguintes afirmações*:

(*i*) $\dim U \leq \dim V$.

(*ii*) *Se* $\dim U = \dim V$, *então* $U = V$.

Prova. Seja B uma base de U. Pela Proposição 6.2.2, existe B' base de V com $B \subset B'$. Assim, $\dim U = |B| \leq |B'| = \dim V$. Se vale que $\dim U = \dim V$, temos que $B = B'$ e assim $U = \operatorname{Span} B = \operatorname{Span} B' = V$. □

6.3. **Dimensão e o algoritmo** Grow**.** Considere o algoritmo Grow (Algoritmo 1) executado com entrada V. Vimos que Grow, se ele termina, ele devolve S linearmente independente tal que $\operatorname{Span} S = V$ (Proposições 5.1.1(*i*) e 5.4.1). Isto é, Grow devolve uma base de V. Vamos agora ver que Grow de fato termina usando o conceito de dimensão.

Proposição 6.3.1. *Suponha que* Grow *é executado com entrada $V \subset \mathbb{F}^D$, onde D é finito. Então a linha* 3 *de* Grow *é executada no máximo $|D|$ vezes. Em particular,* Grow *termina.*

Prova. Sabemos que, ao longo da execução de Grow, o conjunto S é linearmente independente e que S cresce a cada execução da linha 3. Basta agora aplicar a Proposição 6.1.6. □

6.4. **O posto de matrizes.** Dado um conjunto S de vetores de um espaço vetorial, o *posto* de S é $\dim \operatorname{Span} S$. Dada uma matriz $M \in \mathbb{F}^{R \times C}$ o *posto-linha* de M é o posto do conjunto das linhas de M, consideradas como vetores em $\mathbb{F}^C$. O *posto-coluna* de M é o posto do conjunto das colunas de M, consideradas como vetores em $\mathbb{F}^R$.

Proposição 6.4.1. *Para toda matriz $M \in \mathbb{F}^{R \times C}$, seu posto-linha é menor ou igual ao seu posto-coluna.*

Prova. Seja B uma base do espaço das colunas $\operatorname{Span}\{M_{*c} \colon c \in C\}$ de M. Suponha que o posto-coluna de M seja r e suponha $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_r\}$. Seja $P = [\mathbf{b}_1 \mid \cdots \mid \mathbf{b}_r] \in \mathbb{F}^{R \times [r]}$, onde $[r] = \{1, \ldots, r\}$. Pelo fato de B ser base, existe $Q \in \mathbb{F}^{[r] \times C}$ tal que

$$M = PQ. \tag{61}$$

Note agora que (61) implica que as linhas de M pertencem ao espaço $\operatorname{Span}\{Q_{i*} \colon i \in [r]\} \subset \mathbb{F}^C$ gerado pelas r linhas de Q. Assim, o posto-linha de M é no máximo $\dim \operatorname{Span}\{Q_{i*} \colon i \in [r]\} \leq r$. Como r é o posto-coluna de M, obtivemos a desigualdade procurada. □

Corolário 6.4.2. *Para toda matriz $M \in \mathbb{F}^{R \times C}$, seu posto-linha e seu posto-coluna coincidem.*

Prova. Basta aplicar a Proposição 6.4.1 à matriz M e à matriz $M^\top$. □

O *posto* de uma matriz M é o valor comum de seu posto-linha e seu posto-coluna.

6.5. **Soma direta de subespaços vetoriais.** Sejam U e W subespaços de um espaço vetorial V. Quando $U \cap W = \{\mathbf{0}\}$, definimos a *soma direta* $U \oplus W$ de U e W pondo

$$U \oplus W = \{\mathbf{u} + \mathbf{w} \colon \mathbf{u} \in U \text{ e } \mathbf{w} \in W\}. \tag{62}$$

É fácil verificar que $U \oplus W$ é um subespaço vetorial de V (exercício).

Proposição 6.5.1. *A união de uma base de U e uma base de W é uma base de $U \oplus W$. Em particular, se U e W têm dimensão finita, então*

$$\dim U \oplus W = \dim U + \dim W. \tag{63}$$

Prova. Sejam B' e B'' bases de U e W, respectivamente. Seja $B = B' \cup B''$. É simples ver que B gera $U \oplus W$. Vamos agora provar que B é linearmente independente. Para tanto, suponha que uma combinação linear de elementos de B seja igual a $\mathbf{0}$:

$$\alpha_1 \mathbf{b}'_1 + \cdots + \alpha_r \mathbf{b}'_r + \beta_1 \mathbf{b}''_1 + \cdots + \beta_s \mathbf{b}''_s = \mathbf{0}, \tag{64}$$

onde os $\mathbf{b}'_i$ pertencem a B', os $\mathbf{b}''_j$ pertencem a B'', e os α_i e β_j são escalares. Temos então

$$\alpha_1 \mathbf{b}'_1 + \cdots + \alpha_r \mathbf{b}'_r = -\beta_1 \mathbf{b}''_1 - \cdots - \beta_s \mathbf{b}''_s. \tag{65}$$

Entretanto, o lado esquerdo de (65) pertence a U, enquanto que o lado direito de (65) pertence a W. Como $U \cap W = \{\mathbf{0}\}$, deduzimos que ambos os lados de (65) são nulos. Da independência linear de B' e B'', segue que todos os α_i e todos os β_j são nulos. Concluímos que B é linearmente independente.

A identidade (63) segue imediatamente. □

Quando $U \oplus W = V$, dizemos que U e W são subespaços *complementares* de V.

Proposição 6.5.2. *Todo subespaço U de um espaço vetorial V admite um subespaço complementar W em V.*

Prova. Sejam U e V dados como no enunciado. Seja B' uma base de U. Pela Proposição 6.2.2, existe uma base B de V que estende B' (isto é, com $B' \subset B$). Basta tomar $W = \operatorname{Span}(B \setminus B')$ (exercício). □

6.6. **Funções lineares e dimensão.** Seja $f \colon U \to V$ uma função linear. Veremos agora que

$$\dim U = \dim \operatorname{Ker} f + \dim \operatorname{Im} f. \tag{66}$$

Proposição 6.6.1. *Sejam U e V espaços vetoriais e seja $f \colon U \to V$ uma função linear. Existe um subespaço U^* de U tal que*

(*i*) *$U = U^* \oplus \operatorname{Ker} f$ e*

(*ii*) *a função $f^* \colon U^* \to \operatorname{Im} f$ dada por $f^*(\mathbf{u}) = f(\mathbf{u})$ para todo $\mathbf{u} \in U^*$ é bijetora.*

Prova. Seja B' uma base de $\operatorname{Im} f \subset V$ (lembre que $\operatorname{im} f$ é um espaço vetorial). Suponha que $B' = \{\mathbf{b}'_1, \ldots, \mathbf{b}'_r\}$ (o argumento abaixo mostra que B' é finito (exercício)). Escolha $\mathbf{b}_1, \ldots, \mathbf{b}_r \in U$ tais que $f(\mathbf{b}_i) = \mathbf{b}'_i$ para todo i. Seja $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_r\}$ e seja $U^* = \operatorname{Span} B$.

Vamos mostrar que B é linearmente independente. Suponha que $\sum_i \alpha_i \mathbf{b}_i = \mathbf{0}$. Então $\sum_i \alpha_i \mathbf{b}'_i = \sum_i \alpha_i f(\mathbf{b}_i) = f\big(\sum_i \alpha \mathbf{b}_i\big) = \mathbf{0}$. Lembrando que os $\mathbf{b}'_i$ são linearmente independentes, obtemos que todos os α_i são nulos. Concluímos que os $\mathbf{b}_i$ são linearmente independentes, e portanto formam uma base de U^*.

Suponha agora que $\mathbf{u} = \sum_i \alpha_i \mathbf{b}_i$ é tal que $f(\mathbf{u}) = 0$. O argumento acima mostra que todos os α_i são nulos e portanto $\mathbf{u} = \mathbf{0}$ (exercício). Segue que $U^* \cap \operatorname{Ker} f = \{\mathbf{0}\}$ e portanto podemos considerar a soma direta $U' = U^* \oplus \operatorname{Ker} f \subset U$. Vamos mostrar agora que $U' = U$. Fixe $\mathbf{u} \in U$. Seja $\mathbf{v} = f(\mathbf{u}) \in \operatorname{Im} f$. Escrevendo $\mathbf{v}$ na base B', é fácil ver que existe $\mathbf{u}^* \in U^*$ tal que $f(\mathbf{u}^*) = \mathbf{v} = f(\mathbf{u})$. Seja $\mathbf{k} = \mathbf{u} - \mathbf{u}^*$ então $\mathbf{k} \in \operatorname{Ker} f$ e $\mathbf{u} = \mathbf{u}^* + \mathbf{k} \in U^* \oplus \operatorname{Ker} f = U'$. Isto prova que $U \subset U'$ e portanto $U = U'$, isto é, provamos que (*i*) vale.

A verificação de (*ii*) fica como exercício. □

Corolário 6.6.2. *Para qualquer função linear $f\colon U \to V$ com U de dimensão finita, vale a relação* (66).

Prova. Se dois espaços vetoriais A e B são tais que existe uma função linear bijetora $f\colon A \to B$, então A e B tem a mesma dimensão (exercício). Assim, os espaços U^* e $\operatorname{Im} f$ da Proposição 6.6.1 tem a mesma dimensão. Basta agora lembrar (63) e usar (*i*) da Proposição 6.6.1. □

Proposição 6.6.3. *Seja $f\colon U \to V$ uma função linear injetora entre espaços de dimensão finita. Então*

(*i*) $\dim U \leq \dim V$ *e*

(*ii*) *se* $\dim U = \dim V$*, então f é sobrejetora e portanto bijetora.*

Prova. Seja B uma base de U. É fácil ver que a coleção de vetores $f(\mathbf{b})$ com $\mathbf{b} \in B$ é linearmente independente (exercício). Segue que (*i*) vale. Para (*ii*), basta aplicar a Proposição 6.2.3(*ii*) ao subespaço $\operatorname{Im} f$ de V, observando que, por (66), temos que $\dim \operatorname{Im} f = \dim U$ pois supomos f injetora (exercício). □

De fato, a Proposição 6.6.3(*ii*) acima é apenas umas das três implicações no teorema abaixo.

Teorema 6.6.4. *Seja $f\colon U \to V$ uma função linear entre espaços de dimensão finita. Quaisquer duas das três afirmações abaixo implica a terceira*:

(*i*) *f é injetora;*

(*ii*) *f é sobrejetora;*

(*iii*) $\dim U = \dim V$.

Prova. Exercício (use (66)). □

Note que o Teorema 6.6.4 dá critérios necessários e suficientes para f ser inversível, pois f é inversível se e só se valem (*i*) e (*ii*). Por exemplo, deduzimos daquele teorema que se f é inversível, então necessariamente $\dim U = \dim W$ (note que isso não é difícil de se provar diretamente e isso já foi citado na prova do Corolário 6.6.2). Ademais, se f é injetora ou sobrejetora e, além disso, $\dim U = \dim V$, então f é inversível.

6.7. **Matrizes e dimensão.** Seja $A \in \mathbb{F}^{R\times C}$ uma matriz e seja $f_A\colon \mathbb{F}^C \to \mathbb{F}^R$ tal que $f_A(\mathbf{v}) = A\mathbf{v}$ para todo $\mathbf{v} \in \mathbb{F}^C$. Temos que

$$\dim \mathbb{F}^C = \dim \operatorname{Ker} f_A + \dim \operatorname{Im} f_A. \tag{67}$$

Já sabemos que $\dim \mathbb{F}^C = |C|$. Ademais, $\operatorname{Im} f_A = \{A\mathbf{v} \colon \mathbf{v} \in \mathbb{F}^C\}$ coincide com o espaço das colunas $\operatorname{Span}\{A_{*c} \colon c \in C\}$ de A, e portanto $\dim \operatorname{Im} f_A$ é o posto de A. Temos também que $\operatorname{Ker} f_A = \operatorname{Null} A$. Definimos a *nulidade* $\operatorname{nuli} A$ de A como sendo $\dim \operatorname{Null} A = \dim \operatorname{Ker} f_A$. Assim, temos

$$|C| = \operatorname{nuli} A + \operatorname{posto} A. \tag{68}$$

Teorema 6.7.1. *Seja $A \in \mathbb{F}^{R\times C}$ uma matriz. Quaisquer duas das três afirmações abaixo implica a terceira*:

(*i*) $\operatorname{nuli} A = 0$;
(*ii*) $\operatorname{posto} A = |R|$;
(*iii*) $|C| = |R|$.

Ademais, A é inversível se e só se valem quaisquer duas das afirmações acima.

Prova. Exercício. □

6.8. **O aniquilador.** Seja $V \subset \mathbb{F}^n$ um espaço vetorial. O *aniquilador* de V é

$$V^\circ = \{\mathbf{u} \in \mathbb{F}^n \colon \mathbf{u} \cdot \mathbf{v} = \mathbf{0} \text{ para todo } \mathbf{v} \in V\}. \tag{69}$$

É fácil ver que V° é um espaço vetorial. De fato, V° é o espaço nulo de uma certa matriz. Suponha que $\mathbf{a}_i \ldots, \mathbf{a}_r \in \mathbb{F}^n$ formem uma base de V. Seja A a matriz cujas linhas são os vetores linha $\mathbf{a}_i^\top$ $(1 \le i \le r)$:

$$A = \begin{bmatrix} \mathbf{a}_1^\top \\ \vdots \\ \mathbf{a}_r^\top \end{bmatrix} \in \mathbb{F}^{r\times n}. \tag{70}$$

Aqui estamos transpondo os vetores $\mathbf{a}_i \in \mathbb{F}^n$ pois estamos pensando neles como vetores coluna (veja §4.6).

Proposição 6.8.1. *Tem-se que $V^\circ = \operatorname{Null} A$.*

Prova. Isso é imediato, dado que $V = \operatorname{Span}\{\mathbf{a}_1, \ldots, \mathbf{a}_r\}$ e $\mathbf{a}_i^\top \mathbf{u} = \mathbf{u} \cdot \mathbf{a}_i$ (complete os detalhes). □

O seguinte fato segue de (68).

Teorema 6.8.2. *Seja $V \subset \mathbb{F}^n$ um espaço vetorial. Então*

$$\dim V + \dim V^\circ = n. \tag{71}$$

Prova. Como acima, seja $\{\mathbf{a}_i, \ldots, \mathbf{a}_r\}$ uma base de V, e seja A a matriz em (70). Note que $\dim V = r = \operatorname{posto} A$. Ademais, $\dim V^\circ = \dim \operatorname{Null} A = \operatorname{nuli} A$, donde vemos que (71) é equivalente a (68), e o resultado segue. □

Seja $V \subset \mathbb{F}^n$ um espaço vetorial. É fácil ver que $V \subset (V^\circ)^\circ$ (exercício).

Teorema 6.8.3. *Seja $V \subset \mathbb{F}^n$ um espaço vetorial. Então $V = (V^\circ)^\circ$.*

Prova. Já observamos que

$$V \subset (V^\circ)^\circ. \tag{72}$$

Para provarmos que esses dois espaços coincidem, usamos um argumento de dimensão. Aplicando (71) a V e a V°, obtemos

$$\dim V + \dim V^\circ = n \tag{73}$$

e

$$\dim V^\circ + \dim (V^\circ)^\circ = n. \tag{74}$$

Claramente, segue de (73) e (74) que

$$\dim V = \dim (V^\circ)^\circ. \tag{75}$$

Lembrando (*ii*) da Proposição 6.2.3, o resultado segue de (72) e (75). □

6.9. **Representações de espaços vetoriais.** Seja $V \subset \mathbb{F}^D$ um espaço vetorial sobre $\mathbb{F}$. Podemos representar V como $\operatorname{Span} B$, onde B é uma base de V. Há outra forma de se representar V: há necessariamente uma matriz $A \in \mathbb{F}^{R\times D}$ tal que $V = \operatorname{Null} A$. Vamos discutir como obter A a partir de B e vice-versa.

Nossa discussão nessa seção será parcial, no sentido que vamos supor que temos acesso a um algoritmo, Algoritmo X, tal que, dado um espaço vetorial V através de um conjunto gerador B (isto é, tal que $V = \operatorname{Span} B$), devolve uma base para seu aniquilador V°.

Algorithm 10: Algoritmo X

Entrada: Vetores $\mathbf{b}_1, \dots, \mathbf{b}_s \in \mathbb{F}^D$ tais que $V = \operatorname{Span}\{\mathbf{b}_1, \dots, \mathbf{b}_s\}$
Saída: Uma base $\mathbf{a}_1, \dots, \mathbf{a}_r$ do aniquilador $V^\circ \subseteq \mathbb{F}^D$

6.9.1. *De bases para espaços nulos.* Suponha que $V = \operatorname{Span}\{\mathbf{b}_1, \dots, \mathbf{b}_s\}$. Suponha que, alimentando os $\mathbf{b}_i$ ao Algoritmo X, obtemos $\mathbf{a}_1, \dots, \mathbf{a}_r$, que formam um base de V°. Monte a matriz $A \in \mathbb{F}^{R\times D}$ cuja i-ésima linha é $\mathbf{a}_i$ (aqui, $R = \{1, \dots, r\}$). Pela Proposição 6.8.1, temos que $(V^\circ)^\circ = \operatorname{Null} A$. Entretanto, pelo Teorema 6.8.3, temos que $(V^\circ)^\circ = V$ e assim $V = \operatorname{Null} A$. Convertemos assim a representação $V = \operatorname{Span}\{\mathbf{b}_1, \dots, \mathbf{b}_s\}$ para a representação $V = \operatorname{Null} A$.

6.9.2. *De espaços nulos para bases.* Suponha agora que $V = \operatorname{Null} A$ para uma matriz $A \in \mathbb{F}^{R\times D}$. Sejam $\mathbf{a}_i$ ($i \in R$) as linhas de A. Seja $U = \operatorname{Span}\{\mathbf{a}_1, \dots, \mathbf{a}_r\}$. Alimentando esses $\mathbf{a}_i$ ($i \in R$) ao Algoritmo X, obtemos vetores $\mathbf{b}_1, \dots, \mathbf{b}_s$ que formam uma base de U°. Pela Proposição 6.8.1, $U^\circ = \operatorname{Null} A = V$. Assim, os $\mathbf{b}_1, \dots, \mathbf{b}_s$ formam uma base de V, como queríamos.

Observação. Para implementar o Algoritmo X, o que faremos mais à frente é, de fato, resolver o problema "encontrar uma base para $\operatorname{Null} A$" (o problema discutido em §6.9.2) usando eliminação gaussiana.

Sumário